

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

**Applicant:** Wallman

**Conf. No.:** 1382

**Serial No.:** 10/667,852

**Art Unit:** 2134

**Filed:** 9/22/2003

**Examiner:** Tolentino, R

**Title:** **SYSTEM AND METHOD FOR PROVIDING PHYSICAL WEB SECURITY  
USING IP ADDRESSES**

Mail Stop AF  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**PRE-APPEAL BRIEF CONFERENCE REQUEST**

Sir:

Applicant requests a panel of experienced Examiners perform a detailed review of appealable issues for the above-identified patent application pursuant to the Pre-Appeal Brief Conference program. A Notice of Appeal has been filed together with this Request.

Applicant submits that the above-identified application is not in condition for appeal because the Examiner has failed to establish a *prima facie* case of obviousness based on one or more errors in fact.

Applicant respectfully submits that claims 1-4, 6-14 and 16 are allowable because the cited art fails to teach or suggest each and every feature of the claimed invention.

For instance, claim 11 (and similarly claims 1 and 7) recites “comparing the IP address of a *received message* against the list of IP addresses stored by the server.” The Final Office Action never specifically addresses this feature with regard to the grounds of rejection for claim 11. Instead, the Final Office Action states that Sasmazel teaches a physical security system for processing IP address information in order to authenticate the client device in claims 1 and 4 of Sasmazel. This is simply not taught or suggested in Sasmazel. Claims 1 and 4 merely state that an eticket created by the authentication server of Sasmazel includes an IP address. Sasmazel provides no discussion at all of why the IP address is even included in the eticket. However, one skilled in the art would recognize that the IP address is likely provided so that the authorization server can communicate directly back to the client/user to service a request by the end user, e.g., to provide content.

There is no specific teaching, or even suggestion, of comparing the IP address of a received message against a list of IP addresses stored by the server to provide authentication. Instead, Sasmazel teaches away from using the IP address for authentication by specifically stating that authentication information includes, e.g., a “user ID and password” (see, e.g., column 8, lines 24-25). Nowhere does Sasmazel teach using an IP address for authentication purposes.

Note that Sasmazel teaches the use of two servers, an (1) authentication server that determines an identity of a user attempting to access a system (column 1, lines 57-58), and (2) an authorization server that determines what types of activities are permitted for an authenticated user (column, lines 304). As noted above, authentication by the (1) authentication server in Sasmazel is done via a name and password.

Sasmazel neither teaches nor suggests using an IP address for authentication at the (1) authentication server. Any suggestion otherwise is without factual support. Authentication by the (2) authorization server is achieved by successfully decrypting the eticket. "If the hashing technique and public key operate to properly decrypt and rehash the eticket 310, then the information stored in the eticket 310 is determined to be valid." (See column 9, lines 18-20). Once the eticket is determined to be valid (i.e., authentic), then the (2) authorization server can extract the authorization level (see, e.g., column 7, lines 36-37) to determine if the user is authorized for a requested service (see, e.g., column 9, lines 35-49). Thus, neither the (1) authentication server nor the (2) authorization server of Sasmazel teaches or suggests using an IP address for authentication. And clearly, neither server includes a comparing process in which the user's IP address is compared to stored IP addresses.

Sasmazel's invention instead allows an authentication at a first server to be securely packaged in an eticket and sent to a second server in order to avoid having to manually re-authenticate the user at the second server. As noted, Applicant in claim 1 claims a single Internet server that provides both logical authentication (i.e., name and password) and physical authentication (i.e., IP address analysis). It would be counterintuitive for Sasmazel to provide its eticket process in a single server environment such as Applicant's, since the whole purpose of Sasmazel's eticket is to provide secure access to information over a distributed computing environment, such as the web (see, e.g., Summary of the Invention). Nowhere does Sasmazel teach or suggest using both logical and physical authentication at a single server. As noted, the likely purpose of including the IP address in the eticket is so that the authorization

server can communicate back to the user requesting a service. Limiso fails to remedy any of the above deficiencies, as Limiso likewise provides an environment that includes multiple servers.

Accordingly, for these reasons, Applicant submits that claims 1-4, 6-14 and 16 are allowable over the cited art. Claims 5 and 15 are believed allowable for similar reasons. Each of the claims not specifically addressed herein is believed allowable for the reasons stated above, as well as their own unique features. For instance, claim 2 recites “storing a list of each logged in user and a reference IP address collected during a login procedure” (and similarly claim 7). The Final Office Action alleges that this feature is taught in claims 1 and 4 of Sasmazel. However, nowhere does claim 1 or 4 teach storing a list. Claims 1 and 4 merely state that the IP address is included in the ticket, which is specifically encrypted for each user. Nowhere do the cited claims teach storing a *list* of IP addresses for each user logged into the server. Such a suggestion goes beyond any reasonable interpretation of the cited art.

In view of the foregoing, Applicants submit that the Examiner has failed to establish a *prima facie* case under 35 USC 103(a), and that this application is not in condition for appeal and should either be allowed as is, or re-opened for further prosecution.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Michael Hoffman", is written over a horizontal line. The signature is flanked by two small vertical marks, one on each side.

Michael F. Hoffman  
Reg. No. 40,019

Dated: 1/11/2008

Hoffman, Warnick & D'Alessandro LLC  
75 State Street  
Albany, NY 12207  
(518) 449-0044 - Telephone  
(518) 449-0047 - Facsimile